Руководство по интерфейсу командной строки

Плата сетевого управления для 1-фазных и 3-фазных ИБП Easy

AP9544, AP9547

990-91547-028
03/2022

Schneider Electric

Правовая оговорка компании Schneider Electric

Корпорация Schneider Electric не гарантирует надежность, полноту и безошибочность представленной в настоящем руководстве информации. Данное издание не является заменой подробному оперативному плану, разработанному с учетом конкретных условий монтажа. Таким образом, корпорация Schneider Electric не несет никакой ответственности за ущерб, нарушения законов, неправильно выполненный монтаж, сбой системы и другие проблемы, которые могут возникнуть в связи с использованием настоящего издания.

Информация, содержащаяся в настоящей публикации, предоставляется на условиях «как есть» исключительно для планирования дизайна и проектирования центра обработки данных. Информация для данного издания была добросовестно собрана корпорацией Schneider Electric. Однако не дается никакой гарантии, выраженной или подразумеваемой, в отношении полноты и точности представленной в издании информации.

КОРПОРАЦИЯ SCHNEIDER ELECTRIC ИЛИ ЛЮБАЯ ГОЛОВНАЯ ИЛИ ДОЧЕРНЯЯ КОМПАНИЯ ИЛИ ФИЛИАЛ КОРПОРАЦИИ SCHNEIDER ELECTRIC ИЛИ СООТВЕТСТВУЮЩИЕ СЛУЖАЩИЕ, РУКОВОДИТЕЛИ, СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПРЯМЫЕ, КОСВЕННЫЕ, ПОБОЧНЫЕ, ШТРАФНЫЕ, ОСОБЫЕ ИЛИ СЛУЧАЙНЫЕ УБЫТКИ (ВКЛЮЧАЯ, В ТОМ ЧИСЛЕ, УБЫТКИ ИЗ-ЗА УТРАТЫ ПРЕДПРИЯТИЯ, РАСТОРЖЕНИЯ ДОГОВОРА, ПОТЕРИ ВЫРУЧКИ, ДАННЫХ, ИНФОРМАЦИИ ИЛИ ПРЕРЫВАНИЯ ДЕЯТЕЛЬНОСТИ), ВОЗНИКШИЕ В РЕЗУЛЬТАТЕ ИЛИ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ НАСТОЯЩЕГО ИЗДАНИЯ ИЛИ НЕСПОСОБНОСТИ ЕГО ИСПОЛЬЗОВАТЬ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ SCHNEIDER ELECTRIC БЫЛА НЕПОСРЕДСТВЕННО УВЕДОМЛЕНА О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ. КОРПОРАЦИЯ SCHNEIDER ELECTRIC ОСТАВЛЯЕТ ЗА СОБОЙ ПРАВО ИЗМЕНЯТЬ ИЛИ ОБНОВЛЯТЬ СОДЕРЖАНИЕ И ФОРМАТ НАСТОЯЩЕГО ИЗДАНИЯ В ЛЮБОЕ ВРЕМЯ БЕЗ УВЕДОМЛЕНИЯ.

Интерфейс командной строки

Вход в систему

Обзор

Для доступа к интерфейсу командной строки можно использовать локальное подключение (по последовательному каналу связи) или удаленное подключение (Telnet или SSH) с компьютера, находящегося в той же сети, что и плата сетевого управления (ПСУ).

Для доступа к интерфейсу командной строки, который описывается в этом руководстве, на ПСУ должна быть установлена прошивка 1-фазных и 3-фазных ИБП Easy, а сама ПСУ должна быть установлена в поддерживаемый ИБП Easy. Дополнительную информацию о моделях ИБП, совместимых с вашей ПСУ, см. в статье **FA237786** базы знаний на веб-сайте службы технической поддержки APC по адресу **www.apc.com/support**.

Используйте для входа в систему зависящее от регистра имя пользователя и пароль (по умолчанию, **apc** и **apc** для суперпользователя). По умолчанию для пользователя устройства используется имя пользователя **device**. Пользователь с правами только на чтение не имеет доступа к интерфейсу командной строки.

ПРИМЕЧАНИЕ. После первого подключения к ПСУ с учетной записью суперпользователя вам будет предложено ввести новый пароль.

Защитная блокировка. Если правильное имя пользователя используется с неправильным паролем несколько раз (число раз указано в веб-интерфейсе NMC в разделе **Конфигурация > Безопасность > Локальные пользователи > Настройки по умолчанию**), учетная запись пользователя устройства блокируется до повторного включения привилегированным пользователем или администратором.

Информацию об этих параметрах см. в **Руководстве пользователя** платы сетевого управления 3.

Если вы забыли имя пользователя или пароль, см. раздел «Восстановление утерянного пароля» в **руководстве пользователя**.

Удаленный доступ к интерфейсу командной строки

Доступ к интерфейсу командной строки можно выполнять с помощью протокола Telnet или SSH. По умолчанию включен только протокол SSH.

Для включения и отключения этих способов доступа используйте веб-интерфейс. В меню **Консоль управления** выберите **Сеть** > **Консоль > Доступ**.

Кроме того, вы можете включить доступ через Telnet или SSH с помощью интерфейса командной строки. См. раздел «console» на стр. 11.

Протокол SSH для доступа с высоким уровнем защиты. Если для обеспечения надежной защиты веб-интерфейса используется SSL/TLS, для доступа к интерфейсу командной строки нужно использовать протокол SSH.Протокол SSH выполняет шифрование имен пользователей, паролей и передаваемых данных. Вне зависимости от способа доступа к интерфейсу командной строки (SSH или Telnet) интерфейс, учетные записи пользователей и права доступа пользователей остаются неизменными. Однако, чтобы пользоваться SSH, необходимо сначала выполнить настройку и установить на компьютере клиентскую программу SSH.При включении SSH также активируется протокол безопасного копирования SCP (Secure Copy), обеспечивающий защищенную передачу файлов.

1. Используйте следующий пример команды использования SSH для доступа к ПСУ.

   ```
   ssh -c aes256-ctr apc@156.205.14.141
   ```

   ПРИМЕЧАНИЕ. Данная команда SSH предназначена для набора программ OpenSSH. Данная команда может отличаться в зависимости от используемого инструмента SSH.

2. Введите имя пользователя и пароль.

   ПРИМЕЧАНИЕ. После первого подключения к ПСУ с учетной записью суперпользователя вам будет предложено ввести новый пароль.

Протокол Telnet для стандартного доступа. Программа Telnet обеспечивает стандартную аутентификацию по имени пользователя и паролю, однако не имеет преимуществ шифрования, обеспечивающих высокий уровень защиты.

Использование Telnet для доступа к интерфейсу командной строки:

1. На компьютере, который имеет доступ к сети с установленной ПСУ, при приглашении к вводу команды наберите `telnet` и IP-адрес ПСУ (например, `telnet 139.225.6.133`, если ПСУ использует Telnet порт 23 по умолчанию), и нажмите клавишу ENTER.

   ПРИМЕЧАНИЕ. Этот пример применим для командной строки клиентов Telnet. Для разных клиентов Telnet команды могут отличаться.

   Если ПСУ использует номер порта не по умолчанию (от 5000 до 32768), то в зависимости от клиента Telnet необходимо использовать двоеточие или пробел между IP-адресом (или именем DNS) и именем порта. (Эти команды относятся к общему случаю: некоторые клиенты не позволяют указывать порт в качестве аргумента, и для некоторых типов Linux могут потребоваться дополнительные команды).

2. Введите имя пользователя и пароль.

   ПРИМЕЧАНИЕ. После первого подключения к ПСУ с учетной записью суперпользователя вам будет предложено ввести новый пароль.

Локальный доступ к интерфейсу командной строки

Для локального доступа к интерфейсу командной строки используйте компьютер, который подключается к карте сетевого управления через виртуальный последовательный порт USB:

1. С помощью прилагаемого кабеля с интерфейсом micro-USB (номер изделия 960-0603) подключите USB-порт компьютера к порту консоли на плате сетевого управления (ПСУ).
2. В поисковой строке Windows введите Device Manager (Диспетчер устройств) или откройте его из панели управления. Выберите Ports (Порты) и зафиксируйте номер коммуникационного порта, присвоенный ПСУ.
3. Запустите программу терминала (например, такой сторонний эмулятор, как HyperTerminal, PuTTy или Tera Term) и установите следующие значения для коммуникационного порта (зафиксированного в п. 2): 9600 бит/с, 8-битный информационный разряд, без проверки четности, 1 стоповый бит, без контроля потока. Сохраните изменения.
4. Нажмите клавишу ENTER (несколько раз, если требуется) для отображения запроса на ввод **имени пользователя**.
5. Введите имя пользователя и пароль.

   ПРИМЕЧАНИЕ. При первом входе в систему учетная запись привилегированного пользователя будет иметь имя apc. После входа в систему будет предложено ввести новый пароль.

Основной экран

Пример основного экрана

Ниже приведен пример экрана, который отображается при входе в систему с помощью интерфейса командной строки на плате сетевого управления (ПСУ).

```
 Schneider Electric                    Network Management Card AOS  vx.x.x
(c)Copyright 2022 All Rights Reserved Easy UPS 3-Phase APP         vx.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                  Date : 02/30/2022
Contact  : Don Adams                                 Time : 5:58:30
Location : Building 3                                User : Super User
Up Time  : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N4+ N6+ A+
-------------------------------------------------------------------------------
IPv4                 : Enabled          IPv6               : Enabled
Ping Response        : Enabled
-------------------------------------------------------------------------------
HTTP                 : Disabled         HTTPS              : Enabled
FTP                  : Disabled         Telnet             : Disabled
SSH/SCP              : Enabled          SNMPv1             : Read/Write
SNMPv3               : Disabled         Modbus TCP         : Disabled
BACnet/IP            : Enabled
-------------------------------------------------------------------------------
Super User           : Enabled          RADIUS             : Disabled
Administrator        : Disabled         Device User        : Disabled
Read-Only User       : Disabled         Network-Only User  : Read/Write
-------------------------------------------------------------------------------
Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)
apc>
```

Поля информации и состояния

Информационные поля основного экрана.

- Два поля идентифицируют версии операционной системы American Power Conversion (AOS) и версии прошивки приложения (APP). Название прошивки приложения определяет устройство, которое подключается к сети с помощью ПСУ. В приведенном выше примере ПСУ использует прошивку приложения для 3-фазного устройства ИБП Easy.

  ```
  Network Management Card AOS    vx.x.x
  Easy UPS 3-Phase APP           vx.x.x
  ```

- Три поля идентифицируют название системы, контактное лицо и местоположение ПСУ.

  ```
  Name     : Test Lab
  Contact  : Don Adams
  Location : Building 3
  ```

- В поле **«Up Time» (Время работы)** указывается продолжительность работы интерфейса управления ПСУ после последнего запуска или сброса.

  ```
  Up Time : 0 Days 21 Hours 21 Minutes
  ```

- В двух полях указывается дата и время входа в систему.

```
Date : 02/30/2022
Time : 5:58:30
```

- В поле **«User» (Пользователь)** указывается способ входа в систему — с использованием учетной записи **привилегированного пользователя (Super User), администратора (Administrator), диспетчера устройств (Device Manager),** пользователя с правами только на сетевые ресурсы (Network Only) или пользователя с правами только на чтение (Read Only).
  При входе в систему в качестве диспетчера устройств (эквивалент пользователя устройства в интерфейсе пользователя) у вас есть доступ к журналу событий, возможности настройки некоторых параметров ИБП и просмотра ряда активных аварийных сигналов.

```
User : Super User
```

Поля состояния на основном экране.

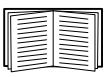
- Поле **Состояние** указывает на состояние ПСУ. Среднее состояние меняется в зависимости от работы выбранного Вами протокола IPv4, IPv6 или обоих, как указано во второй таблице ниже.

```
Stat : P+ N+ A+
```

P+	Операционная система (AOS) работает нормально.

Только IPv4	Только IPv6	IPv4 и IPv6*	Описание
N+	N6+	N4+ N6+	Сеть работает нормально.
N?	N6?	N4? N6?	Выполняется цикл запроса DHCP или BOOTP.
N–	N6–	N4– N6–	ПСУ не подключена к сети.
N!	N6!	N4! N6!	Другое устройство использует IP-адрес платы сетевого управления.
* Значения N4 и N6 могут отличаться: у Вас может быть, например, N4– N6+.			

A+	Приложение работает нормально.
A–	Приложение имеет неправильную контрольную сумму.
A?	Выполняется инициализация приложения.
A!	Приложение несовместимо с операционной системой AOS.



Если P+ не отображается, посетите веб-сайт поддержки клиентов по адресу **http://www.apc.com/site/support/**.

Использование интерфейса командной строки

Обзор

Интерфейс командной строки предусматривает параметры настройки параметров сети и управления ИБП и его платой сетевого управления (ПСУ).

Ввод команд

В интерфейсе командной строки используйте команды для настройки ПСУ. Для выдачи команды наберите команду и нажмите клавишу ENTER. Команды и аргументы можно вводить в нижнем, верхнем и смешанных регистрах. Параметры зависят от регистра.

При использовании интерфейса командной строки можно также выполнять следующие операции.

- Набрать `?` и нажать ENTER, чтобы просмотреть список имеющихся команд на основании типа Вашей учетной записи.

  Для получения информации о назначении и синтаксисе указанной команды наберите команду, пробел и `?` или слово `help`. Например, для просмотра параметра конфигурации RADIUS введите:
  `radius ?`
  или
  `radius help`
- Нажмите клавишу со стрелкой ВВЕРХ для просмотра команды, которая была введена последней в этом сеансе. Используйте клавиши со стрелками ВВЕРХ и ВНИЗ для просмотра списка, в который может входить до десяти команд.
- Наберите по меньшей мере одну букву команды и нажмите клавишу TAB, чтобы просмотреть все команды, которые совпадают с текстом, набранным в командной строке.
- Наберите `ups -st` для просмотра состояния ИБП.
- Введите `exit` или `quit`, чтобы отключить соединение с интерфейсом командной строки.

Синтаксис команды

Пока-затель	**Описание**
-	Параметрам предшествует дефис.
< >	Определения параметров указываются в угловых скобках. Например: `-pw <user password>`
[ ]	Если команда принимает различные параметры или параметр принимает взаимоисключающие аргументы, то значения могут указываться в квадратных скобках.
|	Вертикальная линия между позициями в квадратных или угловых скобках указывает на взаимоисключающие позиции. Необходимо выбрать одну из позиций.

Примеры синтаксиса

Командная строка, которая поддерживает несколько параметров:

```
user -n <имя пользователя> -pw <пароль пользователя>
```

Здесь команда `user` использует два параметра: `-n`, который определяет имя пользователя, и `-pw`, который изменяет пароль.

Например, чтобы изменить пароль на XYZ, введите:

```
user -n apc -pw XYZ
```

ПРИМЕЧАНИЕ. Для привилегированного пользователя также необходимо ввести текущий пароль, если пароль изменяется удаленно. См. раздел «user».

Обратите внимание, что для привилегированного пользователя также необходимо ввести текущий пароль (см. раздел «user»).

Команда, которая принимает для параметра взаимоисключающие аргументы:

```
alarmcount -p [all | warning | critical]
```

В этом примере параметр `-p` принимает только три аргумента: `all`, `warning` или `critical`. Например, для просмотра ряда активных критических аварийных сигналов наберите:

```
alarmcount -p critical
```

Команда не будет выполнена, если введен не указанный аргумент.

Коды реакции на команду

При выполнении заданных операций (скриптов) коды реакции на команду позволяют достаточно точно определять условия ошибки без необходимости точного совпадения с текстом сообщения об ошибке.

Интерфейс командной строки сообщает обо всех командных операциях в следующем формате:

```
E [0-9][0-9][0-9]: Сообщение об ошибке
```

Код	Сообщение об ошибке
E000	Успешно
E001	Успешно задана
E002	Для ввода изменений требуется перезагрузка
E100	Сбой команды
E101	Команда не обнаружена
E102	Ошибка параметра
E103	Ошибка командной строки
E104	Отклонение уровня пользователя
E105	Предварительное заполнение команды
E106	Данные отсутствуют
E107	Потеряна последовательная связь с ИБП
E108	EAPoL выключен из-за недействительного/зашифрованного сертификата

Описание команд

На различных устройствах ИБП могут быть доступны различные команды и параметры из указанных ниже.

Для доступа к некоторым командам, перечисленным ниже, необходимо приобрести лицензию.

Дополнительные сведения см. в документах «**Анализ и определение функциональных возможностей платы сетевого управления для ИБП Easy**» и «**Часто задаваемые вопросы по лицензии**» на веб-сайте APC.

?

Доступ. Привилегированный пользователь, администратор, пользователь устройства.

Описание. Просмотр списка всех команд интерфейса командной строки для учетной записи Вашего типа. Для просмотра текста справки по конкретной команде наберите эту команду и поставьте после нее знак вопроса.

Пример. Для просмотра списка параметров, которые принимаются командой `alarmcount`, наберите:
`alarmcount ?`

about

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение.

Описание. Просмотр информации об аппаратно-программном обеспечении. Эта информация полезна при поиске неисправностей и позволяет определить наличие обновленного аппаратно-программного обеспечения на веб-сайте.

alarmcount

Доступ. Привилегированный пользователь, администратор, пользователь устройства, только для чтения.

Описание.

Параметр	Аргументы	Описание
-p	all	Просмотр ряда активных аварийных сигналов, о которых поступило сообщение с ПСУ. Информация об аварийных сигналах находится в журнале событий.
	warning	Просмотр ряда активных предупреждающих сигналов.
	critical	Просмотр ряда активных критических сигналов.
	informational	Просмотр ряда активных информационных сигналов.

Пример. Для просмотра всех активных предупреждающих сигналов наберите:
`alarmcount -p warning`

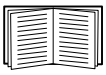
bacnet

Доступ. Привилегированный пользователь, администратор, пользователь устройства.

Описание. Просмотр и настройка параметров BACnet.

BACnet не поддерживается платой AP9544.

Для доступа к этой команде на плате AP9547 требуется лицензия Premium. См. раздел «license».



Дополнительные сведения о точках данных ИБП, предоставляемых посредством BACnet, см. в документах «BACnet Application Maps» (Карты реализации BACnet) на веб-сайте APC www.apc.com.

Параметр	Аргументы	Описание
-S	enable | disable	Выберите этот параметр, чтобы включить или отключить BACnet. Если BACnet отключен, к ПСУ нельзя обратиться через этот протокол. По умолчанию BACnet отключен. **ПРИМЕЧАНИЕ.** Невозможно активировать протокол BACnet, пока не установлен пароль для управления связью с устройством Device Communication Control Password (–pw).
-d	0–4194303	Уникальный идентификатор для устройства BACnet, используемый для обращения к нему.
-n	<имя устройства>	Имя данного устройства BACnet, которое должно быть уникальным в рамках сети BACnet. По умолчанию для устройства используется имя в формате «BACn+последние восемь цифр MAC-адреса ПСУ». Минимальная длина равна 1 символу, максимальная — 150, при этом разрешено использовать специальные символы.
-t	1000–30000	Укажите время ожидания APDU — срок в миллисекундах, в течение которого ПСУ ожидает ответ на запрос BACnet. Стандартное значение — 6000.
-r	0–10	Укажите повторные попытки APDU — число повторных попыток выполнить запрос BACnet, предпринимаемых ПСУ, прежде чем запрос будет прерван. Стандартное значение — 3.
-pw	<пароль>	Служба Device Communication Control используется клиентом BACnet, чтобы дать команду удаленному устройству (например, ПСУ с поддержкой BACnet) прекратить отправлять запросы APDU или отвечать на них (кроме относящихся к службе Device Communication Control) в течение заданного периода. Эту службу можно использовать для диагностики. Укажите пароль Device Communication Control, чтобы клиент BACnet не мог управлять взаимодействием с ПСУ через BACnet, не предоставив заданный здесь пароль. Этот пароль должен иметь длину от 8 до 20 символов и содержать следующее: • Число. • Символ в верхнем регистре. • Символ в нижнем регистре. • Специальный символ. Рекомендуется изменить пароль при первом включении BACnet. Для этого знать текущий пароль не требуется.

Параметр	Аргументы	Описание
Параметры BACnet IP:		
-o	47808, 5000–65535	Укажите порт UDP/IP, используемый ПСУ для отправки и получения сообщений BACnet/IP. **Примечание.** Адрес ПСУ с поддержкой BACnet/IP определяется в виде IP-адреса ПСУ и локального порта.
-fdre	enable | disable	Укажите значение «enable», чтобы зарегистрировать ПСУ на устройстве управления широковещанием BACnet (BBMD). **Примечание.** Вам нужно зарегистрировать ПСУ в качестве стороннего устройства на устройстве BBMD, если в подсети ПСУ сейчас нет устройства BBMD либо ПСУ использует другой локальный порт для BBMD. Дополнительные сведения о регистрации сторонних устройств см. в **руководстве пользователя** ПСУ на **веб-сайте APC**.
-rip	IP-адрес	IP-адрес или полное доменное имя устройства управления широковещанием BACnet, с которым будет зарегистрирована данная ПСУ.
-rpo	5000–65535	Порт устройства BBMD, с которым будет зарегистрирована данная ПСУ.
-fttl	1–65535	Период в секундах, в течение которого BBMD будет считать данную ПСУ зарегистрированным устройством. Если ПСУ не повторит регистрацию до истечения этого срока, BBMD удалит ее из своей таблицы сторонних устройств, после чего ПСУ не сможет отправлять или принимать широковещательные сообщения через это устройство BBMD.
-fsl		Статус регистрации стороннего устройства.

Пример.

```
bacnet
E000: Success
Enabled: yes
Device ID: 1013
Device name: BACnB7D7E5F2
Network Protocol: BACnet/IP
APDU timeout (ms): 6000
APDU retries: 3
IP Port: 47808 (0xBAC0)
Registration Enabled: no
Registration Status: Foreign device registration inactive
Registration BBMD: 0.0.0.0
Registration BBMD port: 47808 (0xBAC0)
Registration TTL: 7200
```

boot

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы

Описание. Настройка того, как ПСУ будет получать свои сетевые параметры, включая IP-адрес, маску подсети и шлюз по умолчанию. После этого требуется настройка параметров сервера BOOTP или DHCP.

Параметр	Аргумент	Описание
-b <режим загрузки>	dhcp | bootp | manual	Определите, как будут настраиваться параметры TCP/IP при включениях, сбросах и перезапусках платы сетевого управления.
-c	enable | disable	Только для режимов загрузки `dhcp`. Включение или отключение требования выдачи сервером DHCP файла cookie APC.
Значения по умолчанию для этих трех настроек обычно менять не требуется:		
-v	<класс поставщика>	APC.
-i	<идентификатор клиента>	MAC-адрес ПСУ, который дает уникальную идентификацию этой платы в сети.
-u	<класс пользователя>	Название модуля микропрограммного обеспечения.

Пример. Чтобы использовать сервер DHCP для получения сетевых параметров, выполните следующие операции.

1. Наберите `boot -b dhcp`
2. Включите требования к серверу DHCP о необходимости выдачи файла cookie APC:
   `boot -c enable`

bye

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение.

Описание. Выход из сеанса интерфейса командной строки. Работает аналогично командам exit и quit.

Пример.

```
bye
Connection Closed - Bye
```

cd

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение.

Описание. Поиск папки в структуре каталога ПСУ.

Пример 1. Для изменения папки `ssh` и подтверждения того, что сертификат безопасности SSH был загружен в ПСУ, выполните следующие операции.

1. Наберите `cd ssh` и нажмите ENTER.
2. Наберите `dir` и нажмите ENTER для получения списка файлов, хранящихся в папке SSH.

Пример 2. Для возврата в предыдущую папку каталога наберите:
`cd ..`

clrrst

Доступ. Привилегированный пользователь, администратор.

Описание. Очистка причины сброса сетевого интерфейса. См. раздел «lastrst» на стр. 18.

console

Доступ. Привилегированный пользователь, администратор, только сеть.

Описание. Определяет, могут ли пользователи иметь доступ к интерфейсу командной строки с помощью протокола Telnet, выключенного по умолчанию, или протокола Secure Shell (SSH), включенного по умолчанию, обеспечивающего защиту путем передачи имен пользователей, паролей и данных в шифрованном виде. Для дополнительной безопасности можно изменить настройку порта Telnet или SSH. Можно также отключить сетевой доступ к интерфейсу командной строки.

Параметр	Аргумент	Описание
`-s`	`enable | disable`	Включение или выключение протокола SSH. При включении протокола SSH включается SCP.
`-t`	`enable | disable`	Включение или выключение протокола Telnet.
`-pt`	`<номер порта telnet>`	Укажите порт Telnet, используемый для связи с ПСУ (по умолчанию 23). Другой диапазон значений: 5000–32768.
`-ps`	`<Номер порта SSH>`	Укажите порт SSH, используемый для связи с ПСУ (по умолчанию 22). Другой диапазон значений: 5000–32768.
`-b`	`2400 | 9600 | 19200 | 38400`	Настройка скорости передачи данных последовательного порта (значение по умолчанию: 9600).

Пример 1. Чтобы обеспечить доступ SSH к интерфейсу командной строки, наберите:
```
console -s
```

Пример 2. Чтобы изменить порт Telnet на 5000, наберите:
```
console -pt 5000
```

date

Доступ. Привилегированный пользователь, администратор.

Описание. Настройте дату, используемую ПСУ.

Сведения о настройке сервера NTP на определение даты и времени для ПСУ см. в **руководстве пользователя**.

Параметр	Аргумент	Описание
-d	<«строка_даты»>	Установка текущей даты. Используйте формат даты, задаваемый командой `date -f`.
-t	<00:00:00>	Настройте текущее время в часах, минутах и секундах. Используйте 24-часовой формат времени.

Параметр	Аргумент	Описание
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Выберите цифровой формат, в котором будут отображаться все даты данного пользовательского интерфейса. Каждая буква m (месяц), d (день) и y (год) представляет один разряд. Однозначные дни и месяцы отображаются с нулем перед значащей цифрой. **ПРИМЕЧАНИЕ.** Формат даты, установленный в настройках пользователя веб-интерфейса ПСУ, переопределит существующую настройку при следующем входе в систему.
-z	<сдвиг часового пояса>	Для определения часового пояса задайте разницу относительно времени по Гринвичу (GMT). Это дает возможность синхронизации с другими людьми в различных часовых поясах.

Пример 1. Для отображения даты в формате гггг-мм-дд наберите:
```
date -f yyyy-mm-dd
```

Пример 2. Чтобы указать дату 30 октября 2009 года в формате, указанном в предыдущем примере, наберите:
```
date -d "30.10.2009"
```

Пример 3. Чтобы задать время 17:21:03, наберите:
```
date -t 17:21:03
```

delete

Доступ. Привилегированный пользователь, администратор.

Описание. Удаление файла в файловой системе. (Сведения об удалении журнала событий см. в **руководстве пользователя**.)

Аргумент	Описание
<имя файла>	Введите название файла, предназначенного для удаления.

Пример. Чтобы удалить файл, выполните следующие действия:

1. Перейдите в папку, в которой находится нужный файл. Например, для перехода к папке журналов `logs` наберите:
   ```
   cd logs
   ```
2. Для просмотра файлов в папке журналов `logs` введите:
   ```
   dir
   ```
3. Наберите
   ```
   delete <имя файла>
   ```

dir

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение.

Описание. Просмотр файлов и папок, хранящихся на ПСУ.

Пример.

```
dir

E000: Success

5165388 Dec 17 2021 apc_hw21_aos_2.1.0.6.bin

  5166412 Jan 17 2021 apc_hw21_eu3p_1.1.0.40.bin

    45000 Dec 17 5:14 config.ini
```

```
0 Feb 23  4:31  db/
0 Feb 23  4:31  ssl/
0 Feb 23  4:31  ssh/
0 Feb 23  4:31  logs/
0 Feb 23  4:31  sec/
0 Feb 23  4:31  fwl/
0 Feb 23  4:31  email/
0 Feb 23  4:31  eapol/
0 Feb 23  4:32  license/
0 Feb 23  4:34  fne/
```

dns

Доступ. Привилегированный пользователь, администратор.

Описание. Настройка и отображение параметров системы доменных имен (DNS) вручную.

Параметр	Аргумент	Описание
-OM	enable | disable	Переопределение ручных настроек DNS.
-y	enable | disable	Синхронизация системы и имени хоста. Работает аналогично параметру «system -s».
-p	<первичный DNS сервер>	Определение первичного DNS-сервера.
-s	<вторичный DNS сервер>	Определение вторичного DNS-сервера.
-d	<имя домена>	Определение имени домена.
-n	<имя домена IPv6>	Определение имени домена IPv6.
-h	<имя хоста>	Установка имени хоста.

Пример.

```
dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

eapol

Доступ. Привилегированный пользователь, администратор.

Описание. Конфигурация настроек EAPoL (Безопасность 802.1 X).

Параметр	Аргумент	Описание
-S	enable | disable	Включение или отключение EAPoL.
-n	<имя запрашивающего устройства>	Задать имя запрашивающего устройства.
-p	<парольная фраза закрытого ключа>	Задать парольную фразу для закрытого ключа.

Пример 1. Для отображения результата команды eapol

```
apc>eapol
E000: Success
Active EAPoL Settings
-------------------
Status:enabled
Supplicant Name:NMC-Supplicant Passphrase:<hidden>
CA file Status:Valid Certificate
Private Key Status:Valid Certificate
Public Key Status:Valid Certificate
Result:Success
```

Пример 2. Чтобы включить EAPoL

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```

email

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Используйте следующие команды для настройки параметров электронной почты, используемых при рассылке уведомлений о событиях с ПСУ.

Для доступа к этой команде требуется лицензия Standard или Premium. См. раздел «license».

Параметр	Аргумент	Описание
-g[n]	<enable | disable>	Включает (по умолчанию) или отключает отправку электронной почты получателю.
-t[n]	<Адрес получателя>	Адрес электронной почты получателя.
-o[n]	<long | short> (формат)	Длинный формат содержит имя, расположение, контакт, IP-адрес, серийный номер устройства, дату и время, код и описание события. Короткий формат содержит только описание события.
-l[n]	<Код языка>	Язык отправляемых сообщений электронной почты. Зависит от установленного языкового пакета.

Параметр	Аргумент	Описание
-r [n]	<Local | recipient | custom> (маршрут)	Установка параметров сервера SMTP: • **Local (Локальный)** (рекомендуется). Выберите этот параметр, если сервер SMTP расположен во внутренней сети или настроен для вашего домена электронной почты. Этот параметр позволяет уменьшить время задержки и количество сбоев сети. При выборе этого параметра необходимо также включить пересылку на сервере SMTP устройства и настроить специальную внешнюю учетную запись для получения пересылаемой электронной почты. **Примечание.** Перед внесением этих изменений обратитесь к администратору сервера SMTP. • **Получатель.** Позволяет отправлять сообщения электронной почты непосредственно на сервер SMTP получателя, который определяется записью MX домена, заданного в адресе получателя. Устройство выполняет только одну попытку отправить сообщение электронной почты. В случае сбоя сети или занятости удаленного сервера SMTP может быть превышено время ожидания и произойдет потеря сообщения. При выборе этого параметра не нужно устанавливать дополнительные административные настройки на сервере SMTP. • **Пользовательский.** Данный параметр позволяет каждому получателю электронной почты иметь собственные настройки сервера. Эти настройки не зависят от устанавливаемых параметром -s[n].
-f[n]	<Адрес отправителя>	Адрес электронной почты, который ПСУ указывает в поле **От кого:** отправляемого сообщения электронной почты.
-s[n]	<Сервер SMTP>	Адрес IPv4/IPv6 или имя DNS локального сервера SMTP. Этот параметр используется, если для параметра -r[n] задано значение «Локальный».
-p[n]	<Порт>	Номер порта SMTP, значение по умолчанию: 25. Альтернативные порты: 465, 587, 2525 и 5000–32768.
-a[n]	<enable | disable> (аутентификация)	Включите этот параметр, если сервер SMTP требует аутентификации.
-u[n]	<Имя пользователя>	Если почтовый сервер требует аутентификации, укажите здесь имя пользователя и пароль.
-w[n]	<Пароль>	
-e[n]	<none | ifsupported | always | implicit> (шифрование)	• **Нет**. Сервер SMTP не требует и не поддерживает шифрование. • **Если поддерживается**. Сервер SMTP объявляет о поддержке STARTTLS, но не требует зашифрованного соединения. Команда STARTTLS отправляется после подачи объявления. • **Всегда**. Сервер SMTP при установлении соединения требует отправки команды STARTTLS. • **Неявно**. Сервер SMTP принимает только зашифрованные соединения. Сообщение STARTTLS не отправляется на сервер.
-c[n]	<enable | disable > (обязательная сертификация)	Этот параметр нужно включить только в том случае, если политика защиты организации не разрешает устанавливать явные доверенные соединения SSL. Если этот параметр включен, действительный корневой сертификат сертифицирующего органа должен быть загружен в ПСУ для шифрования отправляемых сообщений электронной почты.

Параметр	Аргумент	Описание
-i[n]	<Имя файла сертификата>	Данное поле зависит от корневого сертификата сертифицирующего органа, установленного на ПСУ, а также от того, требуется ли корневой сертификат сертифицирующего органа. Файл должен иметь расширение .crt или .cer.
n=	Номер получателя сообщения электронной почты (1,2,3 или 4)	Задает номер получателя электронной почты.

Например: чтобы отправить сообщение получателю 1 с адресом recipient1@apc.com, используя локальный сервер SMTP, введите следующую команду:

```
email -g1 enable -r1 local -t1 recipient1@apc.com
E000: Success
```

eventlog

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение

Описание. Просмотр даты и времени поиска в журнале событий, состояния ИБП и состояния датчиков, подключенных к ПСУ. Просмотр последних событий в устройстве, а также их даты и времени. Для перемещения по журналу событий используются следующие клавиши:

Клавиша	Описание
ESC	Закрытие журнала событий и возврат к интерфейсу командной строки.
ENTER	Обновляется отображение журнала. Используйте эту команду для просмотра событий, которые были записаны после последней операции поиска и отображения журнала.
ПРОБЕЛ	Просмотр следующей страницы в журнале событий.
B	Просмотр предыдущей страницы в журнале событий. Эта команда недоступна на главной странице журнала событий.
D	Удаление журнала событий. Следуйте подсказкам для подтверждения или отклонения удаления. Поиск удаленных событий не выполняется.

exit

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение

Описание. Выход из сеанса интерфейса командной строки.

firewall

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение, отключение или настройка функции внутреннего брандмауэра ПСУ.

Параметр	Аргумент	Описание
-S	<enable | disable>	Включение или выключение брандмауэра.
-f	<имя файла, который необходимо активировать>	Имя файла политики брандмауэра, который необходимо активировать.

Параметр	Аргумент	Описание
-t	<имя файла, который необходимо проверить>	Имя проверяемого брандмауэра, а также время проверки в минутах.
-fe		Вывод списка ошибок активного файла.
-te		Вывод списка ошибок тестового файла.
-c		Отмена проверки брандмауэра.
-r		Вывод списка правил активного брандмауэра.
-l		Вывод журнала активности брандмауэра.
-Y		Пропустите проверочный запрос брандмауэра.

Пример. Чтобы активировать файл политики брандмауэра example.fwl, введите следующую команду:

```
firewall -f example.fwl
E000: Success
```

format

Доступ. Привилегированный пользователь, администратор.

Описание. Переформатирование файловой системы ПСУ и удаление всех сертификатов безопасности, ключей шифрования, параметров конфигурации и журналов событий и данных. Будьте осторожны с этой командой.

Для сброса ПСУ на конфигурацию по умолчанию используйте команду `resetToDef`.

ftp

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение или отключение доступа к серверу FTP. Для дополнительной защиты можно также изменить настройку номера порта на номер любого неиспользуемого порта от 5001 до 32768. Протокол FTP выключен по умолчанию, а протокол Secure CoPy (SCP) включается автоматически при установке пароля для суперпользователя с помощью протокола SSH.

Параметр	Аргумент	Описание
-p	<номер порта>	Определение порта TCP/IP, который используется FTP-сервером для связи с ПСУ (по умолчанию 21). Сервер FTP использует как указанный порт, так и порт с номером на единицу меньше.
-S	enable | disable	Настройка доступа к FTP-серверу.

Пример. Чтобы изменить порт TCP/IP на 5001, наберите:

```
ftp -p 5001
```

help

Доступ. Привилегированный пользователь, администратор, пользователь устройства, только для чтения.

Описание. Просмотр списка всех команд интерфейса командной строки для учетной записи Вашего типа. Для просмотра текста справки по конкретной команде наберите эту команду и поставьте после нее `help`.

Пример 1. Для просмотра списка команд, разрешенных при входе в систему в качестве пользователя устройства, наберите:

```
help
```

Пример 2. Для просмотра списка параметров, которые принимаются командой `alarmcount`, наберите:

```
alarmcount help
```

lang

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на чтение, пользователь с правами только на сетевые ресурсы.

Описание. Используемый язык

Пример.

```
lang
Languages
enUS - English
```

lastrst

Доступ. Привилегированный пользователь, администратор.

Описание. Причина последнего сброса сетевого интерфейса. Результаты выполнения этой команды можно использовать для поиска и устранения неполадок с сетевым интерфейсом при содействии службы технической поддержки.

Параметр	Описание
`02 NMI Reset`	Сброс сетевого интерфейса с помощью кнопки сброса Reset на передней панели ПСУ.
`09 Coldstart Reset`	Сброс сетевого интерфейса из-за отключения питания в оборудовании.
`12 WDT Reset`	Сброс сетевого интерфейса с помощью команды прошивки.

Пример.

```
lastrst
09 Coldstart Reset
E000: Success
```

ledblink

Доступ. Привилегированный пользователь, администратор.

Описание. Создание единого сжатого архива с файлами журнала, доступными на ПСУ и устройстве ИБП. Эти файлы могут использоваться службой технической поддержки для устранения проблем.

Параметры. Время в минутах.

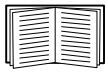
Пример. `ledblink 2`

```
E000: Success
```

license

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Просмотрите сведения о текущей лицензии ПСУ и активируйте лицензию онлайн или автономно.



Дополнительные сведения о лицензиях см. в **руководстве пользователя** интерфейса командной строки платы сетевого управления ИБП Easy и в документе «**Часто задаваемые вопросы о лицензии**», которые доступны на веб-сайте APC.

Параметр	Аргумент	Описание
`-a`	`<Идентификатор активации>`	Идентификатор активации лицензии. Предоставляется в электронном письме от Schneider Electric Exchange при покупке или продлении срока действия лицензии. Его формат: ACT-XXXX-XXXX-XXXX-XXXX.
`-u`	`<URL-адрес сервера>`	Этот URL-адрес используется для связи с сервером лицензирования. Это значение должно быть установлено по умолчанию, чтобы активировать лицензию в Интернете через облачный сервер лицензирования.
`-r`		Запросите файл лицензии на облачном сервере лицензирования.
`-d`		Деактивируйте текущую лицензию.
`-g`		Создайте файл `capabilityRequest.bin`.
`-p`		Обработайте файл `capabilityResponse.bin`.

Пример 1. Чтобы просмотреть сведения о текущей лицензии, введите `лицензию`:

```
E000: Success

License Information

---------------------------------------

License Type:           Standard

Activation Date:        02/14/2022

Expiration Date:        02/13/2023

Activation ID:          ACT-1234-ABCD-5678-EFGH

License Server URL:
https://schneiderelectric.compliance.flexnetoperations.com/deviceservices
```

Пример 2. Чтобы активировать лицензию онлайн, введите:

```
license -a ACT-1234-ABCD-5678-EFGH -r
```

Пример 3. Чтобы активировать лицензию автономно:

1. В интерфейсе командной строки введите: `license -a ACT-1234-ABCD-5678-EFGH -g`.
2. Загрузите файл `capabilityRequest.bin` из ПСУ с помощью SCP или FTP, например: `scp <NMC_username>@<NMC_IP_address>:license/capabilityRequest.bin capabilityRequest.bin`.
3. Зайдите на **Портал лицензий**, войдите в систему, используя свой **Идентификатор активации**, и перейдите в раздел **Устройства > Автономное управление устройствами**. Скачайте файл `capabilityRequest.bin` и загрузите файл `capabilityResponse.bin`.
4. Загрузите файл `capabilityResponse.bin` в ПСУ с помощью SCP или FTP, например: `scp capabilityResponse.bin <NMC_username>@<NMC_IP_address>:license/capabilityResponse.bin`.
5. В интерфейсе командной строки введите: `license -p`.

logzip

Доступ. Привилегированный пользователь, администратор

Описание. Создание единого сжатого архива с файлами журнала, доступными на ПСУ и устройстве ИБП. Эти файлы могут использоваться службой технической поддержки для устранения проблем.

Параметр	Аргумент	Описание
-m	<получатель сообщения электронной почты> (номер получателя от 1 до 4)	Идентификационный номер получателя сообщения электронной почты, которому будет отправлен ZIP-файл. Введите номер одного из четырех настроенных получателей.

Пример.

```
logzip -m 1
Generating files
Compressing files into /dbg/debug_ZA1752123456.tar
Emailing log files to email recipient - 1
E000: Success
```

modbus

Доступ. Привилегированный пользователь, администратор, пользователь устройства.

Описание. Просмотр и настройка параметров функции Modbus.

Для доступа к этой команде требуется лицензия Premium. См. раздел «license».

Параметр	Аргумент	Описание
-tE	<enable | disable> (состояние протокола TCP функции Modbus)	Включение или отключение протокола TCP для функции Modbus.[2]
-tP		Ввод номера порта TCP для функции Modbus. По умолчанию используется порт 502. Допустимые значения: 5000–32768.[2]

Параметр	Аргумент	Описание
-tTo		Укажите время ожидания соединения протокола Modbus TCP в секундах, где 0 указывает на то, что соединение никогда не прерывается. [2]

Пример.

```
modbus
E000: Success
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
Parity = none
TCP Status = ENABLED
TCP Port Number = 502
```

netstat

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Выполняется просмотр состояния сети и всех активных адресов IPv4 и IPv6.

Пример.

```
netstat
Current IP information
Family   mHome    Type     IP Address                          Status
IPv6     4        auto     FE80::2C0:B7FF:FEEA:D325/64         configured
IPv4     0        manual   10.125.43.115/22                    configured
IPv6     0        manual   ::1/128                             configured
IPv4     0        manual   127.0.0.1/32                        configured
```

ntp

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Просмотр и настройка параметров протокола сетевого времени.

Параметр	Аргумент	Описание
-OM	enable | disable	Переопределение ручных настроек.
-p	<первичный сервер NTP>	Укажите первичный сервер.
-s	<вторичный сервер NTP>	Укажите вторичный сервер.
-e	enable | disable	Включение или отключение протокола NTP.
-u	<немедленное обновление>	Немедленное обновление времени ПСУ по NTP-серверу.

Пример 1. Для включения блокировки ручной настройки наберите:
`ntp -OM enable`

Пример 2. Для указания первичного NTP-сервера наберите:
`ntp -p 150.250.6.10`

ping

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы.

Описание. Определяет, подключено ли к сети устройство с указанным IP-адресом или именем DNS. На адрес отправляется четыре запроса.

Аргумент	Описание
<IP-адрес или имя DNS>	Введите IP-адрес в формате *xxx.xxx.xxx.xxx* или имя DNS.

Пример. Чтобы определить, подключено к сети устройство с IP-адресом 150.250.6.10, наберите:
`ping 150.250.6.10`

portspeed

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание.

Параметр	Аргументы	Описание
-s	auto | 10H | 10F | 100H | 100F	Определяется скорость связи с портом Ethernet. Команда `auto` включает устройства Ethernet для согласования передачи с максимально возможной скоростью.

Пример. Чтобы настроить- порт TCP/IP на связь со скоростью передачи 100 Мбит/с в полудуплексном режиме (единовременная связь только в одном направлении), наберите:
`portspeed -s 100H`

ПРИМЕЧАНИЕ. Можно изменить скорость порта до 1000 Мбит/с. Это возможно изменить только в веб-интерфейсе пользователя. Для получения более подробной информации см. пункт «Экран Скорость порта» в **Руководстве пользователя**.

prompt

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы.

Описание. Настройка подсказки интерфейса командной строки для включения или исключения типа учетной записи для текущего пользователя в системе. Любой пользователь может изменить эту настройку; все учетные записи пользователя будут обновлены для использования новой настройки.

Параметр	Аргумент	Описание
-s	long	Подсказка включает в себя тип учетной записи пользователя, находящегося в данный момент в системе.
	short	Настройка по умолчанию. Длина подсказки составляет четыре символа: `apc>`

Пример. Чтобы включить тип учетной записи пользователя, находящегося в данный момент в системе, наберите:

```
prompt -s long
```

pwd

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на чтение, пользователь с правами только на сетевые ресурсы

Описание. Используется для вывода пути к текущему рабочему каталогу.

quit

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на сетевые ресурсы, пользователь с правами только на чтение.

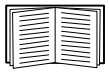
Описание. Закрытие сеанса интерфейса командной строки (работает так же, как и команды exit и bye).

radius

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Просмотр имеющихся параметров RADIUS, включение или отключение аутентификации RADIUS и настройка основных параметров аутентификации, возможная для двух серверов RADIUS.

Для доступа к этой команде требуется лицензия Standard или Premium. См. раздел «license».



Краткое описание конфигурации сервера RADIUS и список поддерживаемых серверов RADIUS приводится в **руководстве пользователя**.

Дополнительные параметры аутентификации для серверов RADIUS см. в интерфейсе пользователя ПСУ.

Дополнительную информацию о настройке сервера RADIUS см. **Security Handbook** (Справочник по защите сети).

Параметр	Аргумент	Описание
-a	local | radiusLocal | radius	Настройка аутентификации RADIUS: `local` — RADIUS отключена. Включена локальная аутентификация. `radiusLocal` — RADIUS, затем локальная аутентификация. Включены RADIUS и локальная аутентификация.Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает или к нему невозможно получить доступ по сети, то используется локальная аутентификация. `radius` — RADIUS включена. Локальная аутентификация отключена.
-p1 -p2 -o1 -o2	<IP-адрес сервера>	Имя сервера или IP-адрес первичного или вторичного сервера RADIUS. **ПРИМЕЧАНИЕ.** По умолчанию серверы RADIUS используют для аутентификации пользователей порт 1812. Чтобы использовать другой порт, добавьте к имени или IP-адресу сервера RADIUS двоеточие с последующим указанием номера нового порта. ПСУ поддерживает порты 1812 и 5000–32768.
-s1 -s2	<секрет сервера>	Разделенный секрет между первичным или вторичным сервером RADIUS и ПСУ.
-t1 -t2	<время ожидания сервера>	Время в секундах, в течение которого плата сетевого управления ожидает ответа от первичного или вторичного сервера RADIUS.

Пример 1.

Для просмотра имеющихся параметров RADIUS для ПСУ наберите `radius` и нажмите клавишу ENTER.

Пример 2. Чтобы включить RADIUS и локальную аутентификацию, наберите:
`radius -a radiusLocal`

Пример 3. Чтобы настроить 10-секундный тайм-аут для вторичного сервера RADIUS, наберите:
`radius -t2 10`

reboot

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Перезапуск интерфейса сетевого управления ПСУ.

Это не влияет на выходное питание устройства, в котором установлена ПСУ.

resetToDef

Доступ. Привилегированный пользователь, администратор.

Описание. Сброс всех настраиваемых параметров на значения по умолчанию.

Параметр	Аргументы	Описание
-p	all | keepip	Внимание! Всем настраиваемым параметрам будут присвоены значения по умолчанию. Выполняется сброс всех измененных параметров, включая действующие события, параметры устройства и, по желанию, параметры конфигурации TCP/IP. Выберите параметр keepip, чтобы сохранить настройки, определяющие способ, которым ПСУ получает значения конфигурации TCP/IP (по умолчанию DHCP).

Команда resetToDef не сбрасывает некоторые параметры, которые недоступны для настройки и могут быть сброшены только путем форматирования файловой системы ПСУ с помощью команды **format**.

Пример. Для сброса всех измененных настроек, *за исключением* параметров TCP/IP для ПСУ, наберите:
`resetToDef -p keepip`

session

Доступ. Привилегированный пользователь, администратор.

Описание. Записывает сведения о выполнившем вход в систему пользователе, интерфейсе, адресе, времени и идентификаторе.

Параметр	Аргументы	Описание
-d	<идентификатор сеанса> (удаление)	Удаление сеанса с указанным идентификатором для текущего пользователя.
-m	<enable | disable> (поддержка многопользовательского режима)	Включите этот параметр, чтобы разрешить одновременный вход в систему нескольких пользователей. Если этот параметр отключен, в систему одновременно может входить только один пользователь.

Параметр	Аргументы	Описание
-a	<enable | disable> (переопределение удаленной аутентификации)	ПСУ поддерживает хранение паролей RADIUS на сервере. Включите переопределение удаленной аутентификации, чтобы разрешить локальным пользователям входить в систему, используя имя и пароль ПСУ, хранящиеся локально в памяти ПСУ.

Пример.

```
session
User     Interface   Address                  Logged In Time        ID
------------------------------------------------------------------------

apc      Telnet      10.169.118.100           00:00:03              19
```

smtp

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Настройка параметров локального сервера электронной почты.

Для доступа к этой команде требуется лицензия Standard или Premium. См. раздел «license».

Параметр	Аргументы	Описание
-f	<Адрес отправителя>	Адрес, с которого ПСУ будет отправлять сообщения электронной почты.
-s	<Сервер SMTP>	Адрес IPv4/IPv6 или имя DNS локального сервера SMTP.
-p	<Порт>	Номер порта SMTP (по умолчанию 25). Возможные значения: 25, 465, 587, 2525, 5000–32768
-a	<enable | disable>	Включите этот параметр, если сервер SMTP требует аутентификации.
-u	<Имя пользователя>	Если почтовый сервер требует аутентификации, укажите здесь имя пользователя и пароль.
-w	<Пароль>	
-e	<none | ifavail | always | implicit>	Параметры шифрования: • **Нет**. Сервер SMTP не требует и не поддерживает шифрование. • **Если доступно**. Сервер SMTP объявляет о поддержке STARTTLS, но не требует зашифрованного соединения. • **Всегда**. Сервер SMTP при установлении соединения требует отправки команды STARTTLS. • **Неявно**. Сервер SMTP принимает только зашифрованные соединения. Сообщение STARTTLS не отправляется на сервер.
-c	<enable | disable>	Необходим корневой сертификат сертификационного органа. Этот параметр нужно включить только в том случае, если политика защиты организации не разрешает устанавливать явные доверенные соединения SSL/TLS. Если этот параметр включен, действительный корневой сертификат сертифицирующего органа должен быть загружен в ПСУ для шифрования отправляемых сообщений электронной почты.

Параметр	Аргументы	Описание
-i	<Имя файла сертификата>	Данное поле зависит от корневого сертификата сертифицирующего органа, установленного на ПСУ, а также от того, требуется ли корневой сертификат сертифицирующего органа.

Пример.

```
From: address@example.com
Server: mail.example.com
Port: 25
Auth: disabled
User: User
Password: <not set>
Encryption: none
Req. Cert: disabled
Cert File: <n/a>
```

snmp

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение или выключение и настройка протокола SNMPv1. По умолчанию протокол SNMPv1 отключен. Необходимо определить имя сообщества (-c[n]) до того, как будет установлена связь с протоколом SNMPv1.

Поддержка SNMP v1 не включена в готовую функциональность. Без лицензии сервисы EcoStruxure будут обнаруживать только ваше устройство; они не могут оказать полную поддержку. Для полной интеграции EcoStruxure приобретите лицензию Standard или Premium, которая включает поддержку SNMP. Дополнительные сведения см. в документах «**Анализ и определение функциональных возможностей платы сетевого управления для ИБП Easy**» и «**Часто задаваемые вопросы по лицензии**» на веб-сайте APC.

В следующей таблице n — это номер управления доступом: 1, 2, 3 или 4.

Параметр	Аргументы	Описание
-S	enable | disable	Включение или выключение протокола SNMPv1.
-c[n]	Сообщество	Указание имени сообщества или строки.
-a[n]	read | write | writeplus | disable	Определение прав на использование.
-n[n]	IP-адрес или имя домена	Указание адреса IPv4/IPv6 или доменного имени для станции сетевого управления.

Пример. Для включения SNMP версии 1 наберите:

```
snmp -S enable
```

snmpv3

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение или выключение и настройка протокола SNMPv3. По умолчанию протокол SNMPv3 отключен. Необходимо активировать действительный профиль пользователя с помощью парольных фраз (-a[n], -c[n]), определенных до того, как будет установлена связь с протоколом SNMPv3.

Поддержка SNMP v3 не включена в готовую функциональность. Без лицензии сервисы EcoStruxure будут обнаруживать только ваше устройство; они не могут оказать полную поддержку. Для полной интеграции EcoStruxure приобретите лицензию Standard или Premium, которая включает поддержку SNMP. Дополнительные сведения см. в документах «**Анализ и определение функциональных возможностей платы сетевого управления для ИБП Easy**» и «**Часто задаваемые вопросы по лицензии**» на веб-сайте APC.

В следующей таблице n — это номер управления доступом: 1, 2, 3 или 4.

Параметр	Аргументы	Описание
-S	enable | disable	Включение или выключение протокола SNMPv3.
-u[n]	<Имя пользователя>	Указание имени пользователя, фразы аутентификации и фразы шифрования.
-a[n]	<Фраза аутентификации>	
-c[n]	<Фраза шифрования>	
-ap[n]	sha | md5 | none	Указание типа протокола аутентификации.
-pp[n]	aes | des | none	Указание протокола защиты (шифрования).
-ac[n]	enable | disable	Включение или выключение доступа.
-au[n]	<Имя профиля пользователя>	Предоставление доступа к указанному профилю пользователя.
-n[n]	<IP-адрес или имя хоста для NMS>	Указание адреса IPv4/IPv6 или имени хоста для станции сетевого управления.

Пример. Для предоставления доступа уровня 2 пользователю «JMurphy» введите:

```
snmpv3 -au2 "JMurphy"
```

snmptrap

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение или отключение создания прерываний SNMP.

Для доступа к этой команде требуется лицензия Standard или Premium. См. раздел «license».

Параметр	Аргументы	Описание
-c[n]	<Сообщество>	Указание имени сообщества или строки.
-r[n]	<IP-адрес ПСУ приемника>	Адрес IPv4/IPv6 или имя хоста приемника прерываний.

Параметр	Аргументы	Описание
-l[n]	<Язык> [код языка]	Выберите язык. Должен быть установлен языковой пакет, содержащий указанный язык. Поддерживаемые коды языков: • enUS — английский • deDe — немецкий • ruRu — русский • zhCn — китайский • jaJa — японский • koKo — корейский • itIt — итальянский • ptBr — португальский • frFr — французский • esEs — испанский
-t[n]	<Тип прерывания> [snmpV1 | snmpV3]	Укажите SNMPv1 или SNMPv3.
-g[n]	<Создание> [enable | disable]	Включение или отключение создания прерываний для данного приемника прерываний. По умолчанию этот параметр включен.
-a[n]	<Аутентификация прерываний> [enable | disable]	Включение или отключение аутентификации прерываний для данного приемника прерываний (только для SNMPv1).
-u[n]	<profile1 | profile2 | profile3 | profile4> (Имя пользователя)	Выберите идентификатор профиля пользователя для данного приемника прерываний (только для SNMPv3).
n = номер приемника прерываний = 1, 2, 3, 4, 5 или 6		

Например: чтобы включить и настроить прерывания SNMPv1 для приемника 1 с именем сообщества public, IP-адресом 10.169.118.100 и английским языком (по умолчанию), введите следующую команду:

```
snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1 snmpV1 -g1 enable
E000: Success
```

ssh

Доступ. Привилегированный пользователь, администратор

Описание. Отобразить, удалить и создать ключи сервера SSH. **ПРИМЕЧАНИЕ.** Доступ к приведенным в таблице ниже параметрам можно получить с помощью команды ssh key.

Параметр	Аргументы	Описание
-s		Отображение текущего используемого ключа сервера SSH.
-f		Отображение текущих отпечатков пальцев ключа сервера SSH.
-d		Удаление текущего используемого ключа сервера SSH.
-i	<Имя файла>.pk15	Импорт ключа сервера SSH из файла № 15 стандарта криптографической защиты с открытым ключом (PKCS).

Параметр	Аргументы	Описание
-ecdsa	256	Создание ключа сервера SSH на основе алгоритма построения электронной цифровой подписи с использованием эллиптических кривых (ECDSA) с указанным размером в битах.
-rsa	1024 | 2048 | 4096	Создание ключа сервера SSH на основе алгоритма криптосистемы Ривеста — Шамира — Адлемана (RSA) с указанным размером в битах.

Пример 1. Для отображения текущего ключа сервера SSH наберите следующее.

```
ssh key -s
E000: Success.
```

Пример 2. Для импорта ключа сервера SSH из файла .p15, генерируемого утилитой NMC Security Wizard CLI (интерфейс командной строки мастера безопасности платы сетевого управления), наберите следующее.

```
ssh key -i nmc.p15
E000: Success.
```

ssl

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы

Описание. Настройка и управление общедоступным ключом ПСУ и сертификатом веб-интерфейса пользователя, а также создание запроса на подпись сертификата (CSR).

ПРИМЕЧАНИЕ. Для данной команды существует три набора параметров, указанные ниже (`key`, `csr`, и `cert`).

Конфигурация настроек общедоступных ключей (`key`):

Параметр	Аргументы	Описание
-s		Отображение текущего используемого общедоступного ключа.
-d		Удаление текущего используемого общедоступного ключа.
-i	<Имя файла>.p15	Импорт общедоступного ключа из файла № 15 стандарта криптографической защиты с открытым ключом (PKCS).
-ecdsa	256 | 384 | 521	Создание общедоступного ключа на основе алгоритма построения электронной цифровой подписи с использованием эллиптических кривых (ECDSA) с указанным размером в битах.
-rsa	1024 | 2048 | 4096	Создание общедоступного ключа на основе алгоритма криптосистемы Ривеста — Шамира — Адлемана (RSA) с указанным размером в битах.

Пример 1. Для создания нового общедоступного ключа ECDSA-521 введите следующее.

```
ssl key -ecdsa 521
```

```
E000: Success.
```

Пример 2. Для импорта общедоступного ключа из файла .p15, генерируемого утилитой NMC Security Wizard CLI (интерфейс командной строки мастера безопасности платы сетевого управления), введите следующее.

```
ssl key -i nmc.p15
```

```
E000: Success.
```

Конфигурация настроек запроса на подпись сертификата (`csr`):

Параметр	Аргументы	Описание
`-s`	`<Имя файла>`	Отображение текущего запроса на подпись сертификата (CSR).
`-q`	`<Имя файла>`	Создание запроса на подпись сертификата (CSR) из активной конфигурации.
`-CN`	`<Общее имя>`	Создание пользовательского запроса на подпись сертификата (CSR). Общее имя является полностью определенным именем домена (FQDN) платы сетевого управления (NMC). Например, именем является его IP-адрес или *.nmc.local.
Параметры пользовательского запроса на подпись сертификата (CSR). **ПРИМЕЧАНИЕ.** Приведенные ниже варианты доступны только для -`CN`.		
`-O`	`<Организация>`	Наименование вашей организации.
`-OU`	`<Подразделение организации>`	Подразделение вашей организации, владеющее сертификатом.
`-C`	`<Страна>`	2-буквенный код страны, в которой находится ваша организация.
`-san`	`<Общее имя | IP-адрес>`	Общее имя или IP-адрес ПСУ.

ПРИМЕЧАНИЕ. Созданные запросы на подпись сертификатов будут храниться в каталоге ssl центра NMC. См. раздел **dir**.

Пример 3. Чтобы создать быстрый запрос на подпись сертификата (CSR) из активной конфигурации, введите следующее.

```
ssl csr -q
```

```
E000: Success
```

Пример 4. Чтобы создать минимальный запрос на подпись сертификата (CSR), введите следующее.

```
ssl csr -CN 190.0.2.0 -C US
```

```
E000: Success
```

Пример 5. Чтобы создать пользовательский запрос на подпись сертификата (CSR), введите следующее.

```
ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local -san 190.0.2.0
```

```
E000: Success
```

Конфигурация настроек сертификата веб-интерфейса пользователя (`cert`):

Параметр	Аргументы	Описание
`-s`	`<Имя файла>`	Отображение указанного сертификата. **ПРИМЕЧАНИЕ.** Выполнение данного параметра без аргумента будет отображать текущий используемый сертификат.
`-f`	`<Имя файла>`	Отображение указанного сертификата отпечатков пальцев. **ПРИМЕЧАНИЕ.** Выполнение данного параметра без аргумента будет отображать текущий сертификат отпечатков пальцев.
`-i`	`<Имя файла>`	Импорт сертификата.

Пример 6. Для отображения активного сертификата введите следующее.

```
ssl cert -s
```

Пример 7. Для отображения файла nmc.crt, расположенного в каталоге ssl, введите следующее.

```
ssl cert -s ssl/nmc.crt
```

Пример 8. Для импорта другого файла other.crt, введите следующее.

```
ssl cert -i other.crt
```

system

Доступ. Привилегированный пользователь, администратор.

Описание. Просмотр и установка имени системы, контактного лица, местоположения и времени работы, а также просмотр даты и времени, текущего пользователя и состояния системы высокого уровня P, N, A (см. раздел «user»).

Параметр	Аргумент	Описание
-n	<имя системы>	Определяется имя устройства, имя ответственного за это устройство и физическое расположение устройства. Примечание. Если для определения значения используется более одного слова, то это значение должно указываться в кавычках. Эти значения используют также StruxureWare Data Center Expert, EcoStruxure IT Expert и агент SNMP ПСУ.
-c	<контакт системы>	
-l	<расположение системы>	
-m	<системное сообщение>	Отображение настраиваемого сообщения или баннера на странице входа веб-интерфейса пользователя или интерфейса командной строки.
-s	enable | disable	Синхронизация системы и имени хоста. Работает аналогично команде «dns -y».

Пример 1. Для определения местоположения устройства как `Test Lab` наберите:

```
system -l "Test Lab"
```

Пример 2. Для задания имени системы `Don Adams` наберите:

```
system -n "Don Adams"
```

tcpip

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Выполняется просмотр и ручная настройка следующих параметров IPv4 TCP/IP для ПСУ:

Параметр	Аргумент	Описание
-S	enable | disable	Включение или выключение TCP/IP v4.
-i	<IPv4-адрес>	Наберите IP-адрес ПСУ, используя формат *xxx.xxx.xxx.xxx*
-s	<маска подсети>	Укажите маску подсети для ПСУ.
-g	<шлюз>	Укажите IP-адрес шлюза, используемого по умолчанию. *Не используйте* шлейфовый адрес (127.0.0.1) в качестве адреса шлюза по умолчанию.
-d	<имя домена>	Укажите имя DNS, сконфигурированное DNS-сервером.
-h	<имя хоста>	Укажите имя хоста, который будет использоваться платой сетевого управления.

Пример 1. Для просмотра сетевых параметров ПСУ наберите `tcpip` и нажмите клавишу ENTER.

Пример 2. Для ручной настройки IP-адреса `150.250.6.10` для ПСУ наберите:
```
tcpip -i 150.250.6.10
```

tcpip6

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение IPv6, просмотр и ручная настройка следующих параметров IPv6 TCP/IP для ПСУ:

Параметр	Аргумент	Описание
-S	enable | disable	Включение или выключение TCP/IP v6.
-man	enable | disable	Разрешение ручной адресации для задания адреса IPv6 ПСУ.
-auto	enable | disable	Разрешение автоматической настройки адреса IPv6 плате сетевого управления.
-i	<адрес IPv6>	Задание адреса IPv6 платы сетевого управления.
-g	<шлюз IPv6>	Задание адреса IPv6 шлюза по умолчанию.
-d6	router | statefull | stateless | never	Задание режима DHCPv6: с управляемыми параметрами маршрутизатора, с сохранением состояния (поддержка состояния для адреса и другой информации), без сохранения состояния (состояние информации, отличной от адреса, не поддерживается), отключение.

Пример 1. Для просмотра сетевых параметров ПСУ наберите `tcpip6` и нажмите клавишу ENTER.

Пример 2. Чтобы вручную настроить адрес Pv6 2001:0:0:0:0:FFD3:0:57ab для ПСУ, наберите:
```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

ups

Некоторые параметры команды **ups** зависят от модели ИБП. В некоторых конфигурациях отдельные параметры команды **ups** могут не поддерживаться.

Доступ. Привилегированный пользователь, администратор, пользователь устройства.

Параметры команды ups для устройств ИБП Easy UPS:

Эти команды доступны только на поддерживаемых 3-фазных устройствах ИБП Easy. Некоторые параметры могут быть доступны только на отдельной модели ИБП. Список устройств ИБП, с которыми совместимы платы сетевого управления, см. в статье базы знаний **FA237786** на веб-сайте **APC**.

Параметр	Аргумент	Описание
-im	<№ фазы> | all	Отображение измерений входных характеристик для выбранной фазы ИБП. При вводе значения all отображаются сведения для всех фаз данного ИБП.
	voltage | current | frequency | all	Указание измерений входных характеристик для команды ups. **Пример:** `ups -input 2 frequency` Отображение значения частоты для фазы 2 данного ИБП.
-bym	<№ фазы> | all	Отображение измерений входных характеристик для выбранной фазы сети байпаса. При вводе значения all отображаются все фазы сети байпаса.
	voltage | current | frequency | all	Указание измерений входных характеристик для команды ups. **Пример:** `ups -bypass 2 current` Отображение тока для фазы 2 сети байпаса.
-om	<№ фазы> | all	Отображение измерений выходных характеристик для выбранной фазы данного ИБП. При вводе значения all отображаются сведения для всех фаз данного ИБП.
	voltage | current | load | power | percload | pf | frequency | all	Указание измерений выходных характеристик для команды ups. **Пример:** `ups -output 2 percload` Отображение процента нагрузки для фазы 2 данного ИБП.
-bat		Отображение состояния батареи ИБП.
-abt		Отображение сведений об ИБП.
-al	c | w | i	Отображение всех имеющихся сигналов тревоги. При вводе значений c, w или i отображаются только критические (c), только предупредительные (w) или только информационные (i) сигналы тревоги.
-amb		Отображение температуры окружающей среды данного ИБП.
-maint		Отображение параметров обслуживания данного ИБП.

Пример 1. Для просмотра параметров обслуживания введите следующее.

```
ups -main
```

Эти команды доступны только на поддерживаемых 1-фазных устройствах ИБП Easy. Некоторые параметры могут быть доступны только на отдельной модели ИБП. Список устройств ИБП, с которыми совместимы платы сетевого управления, см. в статье базы знаний **FA237786** на веб-сайте **APC**.

Параметр	Описание
-im	Отображение входных характеристик ИБП: входного напряжения, входного аварийного напряжения и частоты.
-om	Отображение выходных характеристик ИБП: выходного напряжения, выходного тока, номиналы активной мощности и полной мощности.
-bat	Отображение характеристик батареи ИБП: напряжения и температуры батареи.
-al	Отображение всех имеющихся критических, предупредительных и информационных сигналов тревоги.
-abt	Отображение сведений об ИБП.

Пример 2. Для просмотра входных характеристик введите следующее.

```
ups -im

E000: Success

UPS Input Measurement(s)

-----------------------

Voltage:       245.7 VAC

Frequency:     59.99 Hz

Fault Voltage: 200.0 VAC
```

user

Доступ. Привилегированный пользователь, администратор.

Описание. Задание имени пользователя и пароля для каждого типа учетной записи, а также задание времени ожидания отсутствия активности. (Имя пользователя изменить нельзя. Необходимо удалить, а затем создать нового пользователя.)

Дополнительную информацию о разрешенных действиях для каждого типа учетной записи (привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на чтение и пользователь с правами только на сетевые ресурсы) см. в **руководстве пользователя**.

Параметр	Аргумент	Описание
-n	<пользователь>	Укажите пользователя.
-cp	<текущий пароль>	Для привилегированного пользователя необходимо указать текущий пароль. **ПРИМЕЧАНИЕ.** Параметр -cp требуется, только если пароль привилегированного пользователя изменяется удаленно.
-pw	<пароль пользователя>	Укажите эти параметры для пользователя. **ПРИМЕЧАНИЕ.** Описание необходимо заключить в кавычки.
-pe	<разрешение пользователя>	
-d	<описание пользователя>	
-e	enable | disable	Включение или отключение доступа к определенной учетной записи пользователя.
-te	enable | disable	Включение доступа к сенсорному экрану.
-tp	<pin-код доступа к сенсорному экрану>	Еще не реализовано.

Параметр	Аргумент	Описание
-tr	enable | disable	Включение переопределения удалённой авторизации сенсорного экрана. Этот параметр доступен только на некоторых устройствах. Если включить это переопределение, ПСУ позволит локальному пользователю выполнить вход с помощью пароля для ПСУ, сохраненного локально на ПСУ.
-st	<время ожидания сеанса>	Укажите время ожидания сеанса перед выходом пользователя при отсутствии активности его клавиатуры.
-sr	enable | disable	Режим обхода функций RADIUS при использовании последовательного соединения консоли (CLI) также называется переопределением аутентификации удаленного последовательного интерфейса.
-el	enable | disable	Определение цветовой кодировки журнала событий.
-lf	tab | csv	Определение формата экспорта файла журнала.
-ts	us | metric	Определение шкалы температуры (шкала по Фаренгейту или Цельсию).
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Указание формата даты.
-lg	<код языка (например, enUs)>	Укажите язык пользователя. Для просмотра списка доступных языков и соответствующих языковых кодов введите команду lang.
-del	<имя пользователя>	Удаление пользователя.
-l		Отображение текущего списка пользователей.

Пример. Чтобы изменить время выхода из системы для пользователя JMurphy, установив его на 10 минут, наберите:

```
user -n “JMurphy” -st 10
```

userdflt

Доступ. Привилегированный пользователь, администратор.

Описание. Эта функция дополняет параметр «user» и позволяет задать предпочтения пользователя по умолчанию. Настройки пользователя по умолчанию выполняют две основные функции:

- Определение значений по умолчанию, которые вводятся во все поля при создании нового пользователя администратором или привилегированным пользователем. Эти значения можно изменить до того, как настройки будут применены к системе.
- Для удаленных пользователей, учетные записи которых не хранятся в системе и проходят удаленную аутентификацию (например, по протоколу RADIUS), эти значения используются вместо тех, которые не были предоставлены сервером аутентификации.

Например, если сервер RADIUS не предоставляет предпочтительное значение температуры для пользователя, будет использоваться значение, определенное в этом разделе.

Параметр	Аргумент	Описание
-e	<enable | disable> (включение)	Пользователь будет по умолчанию включен или отключен при создании. Удалите фразу (Включение) из конца строки.
-pe	<Administrator | Device | Read-Only | Network-Only> (разрешение пользователя)	Указание уровня разрешений и типа учетной записи пользователя.
-d	<описание пользователя>	Ввод описания пользователя. Описание необходимо заключить в кавычки.

Параметр	Аргумент	Описание
-st	<время ожидания сеанса> в минутах	Указание времени ожидания сеанса по умолчанию.
-bl	<число неудачных попыток входа>	Число неудачных попыток входа, по достижении которого система отключит учетную запись пользователя. В этом случае будет показано сообщение с уведомлением о блокировке учетной записи. Чтобы разблокировать такую учетную запись и восстановить возможность входа в систему, требуется учетная запись с правами привилегированного пользователя или администратора. **ПРИМЕЧАНИЕ.** Учетная запись привилегированного пользователя не блокируется, но при необходимости может быть отключена вручную.
-el	<enable | disable> (Цветовая кодировка журнала событий)	Включение или отключение цветовой кодировки событий.
-lf	<tab | csv> (Формат журнала экспорта)	Укажите формат журнала экспорта (файл с разделителями символами табуляции или CSV).
-ts	<us | metric> (Температурная шкала)	Укажите температурную шкалу пользователя. Этот параметр также используется системой в том случае, если недоступна предпочтительная настройка пользователя (например, уведомления по электронной почте).
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyymm-dd> (Формат даты)	Укажите предпочтительный формат даты для пользователя.
-lg	<код языка (например, enUs)>	Указание языка пользователя. Для просмотра списка доступных языков и соответствующих языковых кодов введите команду lang.
-sp	<enable | disable>	Включение или отключение надежных паролей.
-pp	<Интервал в днях>	Интервал, через который осуществляется обязательная смена пароля.

Пример. Чтобы установить для пользователя время ожидания сеанса по умолчанию, равное 60 минутам, введите следующую команду:

```
userdflt -st 60
E000: Success
```

web

Доступ. Привилегированный пользователь, администратор, пользователь с правами только на сетевые ресурсы.

Описание. Включение доступа к интерфейсу пользователя с использованием протоколов HTTP и HTTPS.

Для дополнительной безопасности можно изменить настройку порта для HTTP и HTTPS, задав любой неиспользуемый порт от 5000 до 32768. Пользователи должны использовать двоеточие (:) в адресном поле браузера для указания номера порта. Например, для номера порта 5000 и IP-адреса 152.214.12.114:
`http://152.214.12.114:5000`

Параметр	Аргумент	Описание
-h	enable | disable	Включение или выключение доступа к интерфейсу пользователя для протокола HTTP. По умолчанию протокол HTTP отключен.
-s	enable | disable	Включение или выключение доступа к интерфейсу пользователя для протокола HTTPS. По умолчанию параметр HTTPS отключен. При включении HTTPS данные шифруются во время передачи и аутентифицируются цифровым сертификатом с помощью SSL/TLS.

Параметр	Аргумент	Описание
-mp	<минимальный протокол>	Указание минимального протокола, который использует веб-интерфейс: SSL версии 3.0, TLS версии 1.1 или TLS версии 1.2.
-ph	<http порт №>	Указывается порт TCP/IP, используемый HTTP для связи с ПСУ (по умолчанию 80). Другой диапазон доступных значений: 5000–32768.
-ps	<https порт №>	Указывается порт TCP/IP, используемый HTTPS для связи с ПСУ (по умолчанию 443). Другой диапазон доступных значений: 5000–32768.
-lsp	enable | disable	Включение или отключение доступа к странице ограниченного состояния в веб-интерфейсе пользователя.
-lsd	enable | disable	Включение или отключение использования страницы ограниченного состояния в качестве страницы по умолчанию при доступе к IP-адресу или имени хоста устройства в веб-браузере.
-cs	<0 | 1 | 2 | 3 | 4>	Выберите уровень безопасности от 0 до 4 для наборов шрифтов TLS v1.2, где 4 — высший уровень безопасности, а 0 — низший уровень безопасности. Стандартное значение — 4. **ПРИМЕЧАНИЕ.** Параметр – cs применим только, когда параметр – mp установлен для TLS v1.2. После ввода значения от 0 до 4 интерфейс командной строки выдает ответ в виде списка разрешенных наборов шрифтов SSL.

Пример. Чтобы заблокировать любой доступ к интерфейсу пользователя по протоколу HTTPS, введите:

```
web -s disable
```

whoami

Доступ. Привилегированный пользователь, администратор, пользователь устройства, пользователь с правами только на чтение, пользователь с правами только на сетевые ресурсы.

Описание. Предоставляет сведения для входа в систему для текущего пользователя.

Пример.

```
apc> whoami
E000: Success
apc
```

wifi

Доступ. Привилегированный пользователь, администратор

Описание. Включение или отключение Wi-Fi и изменение настроек сети Wi-Fi. **ПРИМЕЧАНИЕ.**

Для выполнения данной команды требуется, чтобы дополнительное устройство APC USB Wi-Fi (AP9834) было вставлено в USB-порт платы AP9544/AP9547.

ВАЖНО: Не рекомендуется загружать целый файл config.ini, взятый с устройства с проводным соединением, на устройство, подключеное по Wi-Fi. Также не рекомендуется загружать целый файл config.ini, взятый с устройства, подключенного по Wi-Fi, на устройство с проводным соединением, если только весь раздел `[NetworkWiFi]` не будет удален или закомментирован с помощью точки с запятой (например, `;WiFi = enabled`).

Раздел `[NetworkWiFi]` содержит настройки устройства, специфичные для использования Wi-Fi. Эти настройки не следует выгружать на устройство с проводным соединением.

Параметр	Аргумент	Описание
`-S`	`enable | disable`	Включение или отключение Wi-Fi. По умолчанию этот параметр имеет значение disable (выключено). **ПРИМЕЧАНИЕ.** Включение/отключение Wi-Fi отключит/включит проводное соединение по локальной сети.
`-n`	`<Сетевое имя (SSID)>`	Укажите сетевое имя (SSID) сети Wi-Fi. Максимальная длина — 32 символа.
`-t`	`WPA | WPA2-AES | WPA2-Mixed | WPA2-TKIP | WPA2-Enterprise`	Укажите тип безопасности (аутентификация и шифрование) сети Wi-Fi.
`-p`	`<Пароль wi-fi>`	Укажите пароль для сети Wi-Fi. Максимальная длина — 64 символа. **ПРИМЕЧАНИЕ.** Данный параметр необходим для безопасности типов WPA, WPA2-AES и WPA2-Mixed.
`-eu`	`<Имя пользователя WPA2-Enterprise>`	Имя пользователя для аутентификации в среде WPA2-Enterprise. Максимальная длина — 32 символа.
`-ep`	`<Пароль WPA2-Enterprise>`	Пароль для аутентификации в среде WPA2-Enterprise. Максимальная длина — 32 символа.
`-eo`	`<Внешняя идентификация WPA2-Enterprise>`	Укажите внешнюю идентификацию WPA-2-Enterprise. Это дополнительная нешифрованная идентификация, используемая сервером WPA-2-Enterprise. Например: user@example.com или анонимно. Максимальная длина — 32 символа.
`-fw`	`<Путь/имя_файла>`	Укажите файл прошивки для обновления прошивки устройства APC USB Wi-Fi. Это должен быть файл .ism, расположенный на USB-накопителе, который вставлен в USB-порт центра NMC. **ПРИМЕЧАНИЕ.** Во время обновления прошивки сеть Wi-Fi будет недоступна.

Пример 1. Для включения Wi-Fi и изменения настроек сети Wi-Fi введите следующее.

```
wifi -S enable -n NETGEAR06 -t WPA2-AES -p apc123
```

Пример 2. Для обновления прошивки устройства APC USB Wi-Fi введите следующее.

```
wifi -fw apc_uw01_wni_1-26-7.ism
```

xferINI

Доступ. Привилегированный пользователь, администратор. Эта команда работает только через последовательный интерфейс командной строки или локальную консоль.

Описание. Использование XMODEM для загрузки .ini файла при доступе к интерфейсу командной строки через последовательный канал связи. После завершения загрузки:

- Если система или сеть изменились, то происходит перезапуск интерфейса командной строки, и необходимо заново войти в систему.
- Если для передачи файлов выбрана скорость в бодах, которая отличается от скорости передачи ПСУ по умолчанию, то для установки связи с ПСУ необходимо переустановить значение скорости на значение по умолчанию.

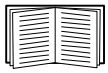
xferStatus

Доступ. Привилегированный пользователь, администратор.

Описание. Просмотр результатов последней передачи файла.

Пример. `xferStatus`

```
E000: Success
Result of last file transfer: OK
```



Описание кодов результатов передачи приведено в **руководстве пользователя**.

Уведомления об авторских правах

Криптологическая библиотека Cryptlib

База данных Беркли

Распространение и использование в исходном и двоичном виде с изменением или без такового разрешено только при соблюдении следующих условий.

1. Распространение исходного кода должно учитывать вышеуказанные заявления об авторских правах, перечень условий и следующие ограничения.
2. Распространение в двоичном виде должно учитывать вышеуказанные заявления об авторских правах, перечень условий и следующие ограничения в документации и других материалах, предоставленных для распространения.
3. Рекламные материалы, упоминающие характеристики и использование настоящего программного обеспечения, должны признавать следующее. Этот продукт содержит программное обеспечение, разработанное Калифорнийским университетом в Беркли и его сотрудниками.
4. Название университета и имена его сотрудников не должны использоваться для поддержки и продвижения продуктов, созданных на основе данного программного обеспечения без предварительного письменного разрешения.

ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО РУКОВОДСТВОМ И СОТРУДНИКАМИ НА УСЛОВИЯХ «КАК ЕСТЬ», И, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ЛЮБЫЕ ЯВНО ВЫРАЖЕННЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ ПРОДАЖИ И СООТВЕТСТВИЯ КОНКРЕТНЫМ ЦЕЛЯМ НЕПРИМЕНИМЫ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ РУКОВОДСТВО ИЛИ СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ НИ ЗА КАКИЕ ПРЯМЫЕ, НЕПРЯМЫЕ, СЛУЧАЙНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, ПОМИМО ПРОЧЕГО, ПРИОБРЕТЕНИЕ ТОВАРОВ ИЛИ УСЛУГ НА ЗАМЕНУ, ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ ИЛИ ПРИОСТАНОВКУ БИЗНЕСА) ПО ЛЮБОЙ ПРИЧИНЕ И ПО ЛЮБОЙ ТЕОРИИ ОТВЕТСТВЕННОСТИ, ОБЯЗАТЕЛЬСТВАМ, ВЫРАЖЕННЫМ В КОНТРАКТЕ, СТРОГИМ ОБЯЗАТЕЛЬСТВАМ, ИЛИ ПРИ ГРАЖДАНСКОМ ПРАВОНАРУШЕНИИ (ВКЛЮЧАЯ ХАЛАТНОСТЬ И ПРОЧЕЕ), ВОЗНИКАЮЩИЕ КАКИМ БЫ ТО НИ БЫЛО ОБРАЗОМ ВСЛЕДСТВИЕ ПРИМЕНЕНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ПРИ НАЛИЧИИ ИНФОРМАЦИИ О ВОЗМОЖНОСТИ НАНЕСЕНИЯ ДАННОГО УЩЕРБА.

Lua

Настоящим бесплатно предоставляется разрешение любому лицу, получающему копию этого программного обеспечения и связанных с ним файлов документации («Программное обеспечение»), работать с программным обеспечением без ограничений, включая, помимо прочего, права на использование, копирование, изменение, слияние, публикацию, распространение, сублицензирование и/или продажу копий программного обеспечения, а также разрешать лицам, которым предоставляется программное обеспечение, делать это, при соблюдении следующих условий.

Приведенное выше уведомление об авторских правах и настоящее уведомление о разрешении должны быть включены во все копии или существенные части программного обеспечения.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ГАРАНТИЯМИ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И НЕНАРУШЕНИЯ ПРАВ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ АВТОРЫ ИЛИ ПРАВООБЛАДАТЕЛИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПРЕТЕНЗИИ, УБЫТКИ ИЛИ ДРУГИЕ ОБЯЗАТЕЛЬСТВА, БУДЬ ТО В СВЯЗИ С ДОГОВОРНЫМ, ДЕЛИКТНЫМ ИЛИ ИНЫМ ОБРАЗОМ, ВОЗНИКАЮЩИЕ ИЗ ИЛИ В СВЯЗИ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ, ИЛИ ИСПОЛЬЗОВАНИЕМ, ИЛИ ДРУГИМИ СДЕЛКАМИ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

Глобальная служба технической поддержки компании APC корпорации Schneider Electric

Пользовательская поддержка данного или любого другого изделия осуществляется бесплатно одним из следующих способов:

- Обратитесь на сайт компании Schneider Electric для доступа к документам базы знаний Schneider Electric и отправки запроса на обслуживание.
  - **www.apc.com** (центральное отделение)
    Обратитесь на локализованные для отдельных стран веб-сайты корпорации Schneider Electric, на каждом из которых содержится информация о технической поддержке.
  - **www.apc.com/support/**
    Глобальная техническая поддержка с помощью поиска в базе знаний компании Schneider Electric и использование системы электронной поддержки.
- Обратитесь в центр технической поддержки компании Schneider Electric по телефону или по электронной почте.
  - Региональные центры: см. контактную информацию на веб-сайте **www.apc.com/support/contact**.

Информацию о местных центрах технической поддержки можно также получить у представителя или у дистрибьютора, у которого было приобретено изделие.

990-91547-028 03/2022